Adversary Models in Wireless Networks: Research Challenges

Radha Poovendran
Network Security Lab (NSL)
University of Washington

Questions Posed by the Committee

- What are the three fundamental limitations of today's security mechanisms?
- What are the three most important research challenges?
- What are promising innovations and abstractions for future systems?
- What are possible milestones for the next 5 to10 years?

Three fundamental limitations of today's security mechanisms

- Refer to Virgil's presentation
- Force-fitting the old models into the wireless environment
- Considering security as an overlay instead of a critical robustness requirement
- Optimizing network performance independently of security

Most Important Challenges

- Identifying the primitives that can be used to characterize adversary models
  - Characterize space of attacks against the network operations
  - Incorporate resource constraints for the adversary (mobility, computation, stealthiness, multiple presence)
  - Address adaptive (intelligent) as well as mobile adversary
  - Differentiate selfish vs. malicious behavior and network faults
- Defining suitable security metrics
  - To quantify the impact of an attack on the network or individual nodes
  - To couple the network performance with security
  - Flexible enough to incorporate cross-layer impact while being adaptive to attacks
- Not Ignoring the fact that in large scale networks, statistics often beat out carefully designed attacks (such as MITM)—Leading to "Passive attacks of probabilistic nature may be resource and computationally efficient than active attacks in WSN/RFID."
- Designing security protocols that leak minimal side information!

Promising innovations and abstractions

- Graph abstractions
  - Network connectivity, Throughput
  - Robustness to intelligent attacks
- Probabilistic Analysis Techniques for
  - Modeling attacks
  - Quantifying the impact of attacks
  - Tuning defense strategy
- Potential New Primitives (More from Peng, Adrian)
- New Approaches in Network Optimization

Possible milestones for the next 5 to10 years

- Joint design of performance and security
- Development of performance metrics
  - Characterizing/Knowing the limitations of our solutions
- Adversarial models and extensions of them for
  - Heterogeneous environments
  - Resource as well as location adaptive attacks
- Also need breakthrough in new crypto primitives
  - Lightweight, suitable for resource constrained devices

Final Thoughts

- Biggest Limitation: Security is considered as an afterthought, decoupled from network performance
- Biggest Challenge: Define cross-layer security/performance metrics and realistic attack models
- Final Goal: Span the space of attacks and quantify their impact